STATEMENT OF

JOSEPH S. MAHALEY

DIRECTOR, OFFICE OF SECURITY

DEPARTMENT OF ENERGY

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, EMERGING THREATS, AND

INTERNATIONAL RELATIONS

COMMITTEE ON GOVERNMENT REFORM

U. S. HOUSE OF REPRESENTATIVES

JUNE 24, 2003

Thank you, Mr. Chairman, I appreciate this opportunity to provide the committee with information concerning the Department of Energy's recently completed efforts to update its Design Basis Threat.

The Department of Energy (DOE) recently revised its Design Basis Threat Policy in 2003 to reflect changes in perceived threats to United States government assets and operations. The new Design Basis Threat Policy, approved in May 2003, is designed to reflect the most credible threats to Departmental assets and operations and provide a baseline for operational and budgetary planning purposes. The DOE Design Basis Threat Policy is derived from and associated with national intelligence threat information and other government agencies' threat policy statements.

The 2003 DOE Design Basis Threat Policy is predicated on the information contained in the Defense Intelligence Agency, "Postulated Threat: to U.S. Nuclear Weapons Facilities and other Selected Strategic Facilities," dated January 2003, also referred to as the Postulated Threat Statement. The Postulated Threat Statement details relevant threat information about postulated adversary team sizes, characteristics, capabilities and applicability to national security assets. The Postulated Threat Statement is based on intelligence information detailing actual terrorist attacks and the equipment and tactics utilized in the attacks, expert judgments regarding stated terrorist intentions and the ability of the terrorist to execute the stated objectives, and postulated capabilities based on the latest knowledge concerning terrorist activities.

Prior to the September 11, 2001, attacks in New York and Washington, the Department of Energy, in August 2001, requested that the intelligence community prepare an update to the 1994 Postulated Threat Statement. Although the 1994 Postulated Threat Statement was designed to be a 10-year document, we believed at that time that changes in international politics, emerging technologies and increases in worldwide terrorism required a reassessment. The National Intelligence Coordinating Committee assigned the primary responsibility for updating the Postulated Threat Statement to the Defense Intelligence Agency.

The events of September 11, 2001, delayed the Postulated Threat Statement update effort due to reallocation of critical assets. However, the requested Postulated Threat Statement update was fully underway by January 2002. The primary entities collaborating on the revision to the Postulated Threat Statement were: the Defense Intelligence Agency, the Department of the Navy, the Department of the Army, the Department of the Air Force, the Nuclear Regulatory Commission, the Federal Bureau of Investigation, the Central Intelligence Agency, and the Department of Energy.

The Department of Energy's Office of Security began revising the DOE Design Basis Threat Policy in October 2001. Our work on the revised DOE Design Basis Threat Policy was carried out in parallel with the work on the updated Postulated Threat Statement to reduce the amount of time that would be required to issue a final DOE Design Basis Threat Policy upon completion of the Postulated Threat Statement. After the release of the final Postulated Threat Statement in January 2003, we made final revisions to the Departmental Design Basis Threat Policy. The

Policy was then coordinated within the Department of Energy, including the National Nuclear Security Administration. The revised Policy was approved by the Deputy Secretary of Energy on May 20, 2003.

The new Design Basis Threat Policy will provide managers an improved threat policy document to plan, resource, and execute vital safeguards and security programs. In addition to updated threat information, the revised Design Basis Threat Policy includes a significant enhancement over prior policies - the use of the "graded threat concept". The graded threat concept considers and accounts for factors such as consequences of a malevolent event, the attractiveness of the asset, the ability of an adversary to accomplish a given objective with an asset, and the resources required by an adversary to accomplish a given objective.

The graded threat approach includes the establishment of "Threat Levels" for Departmental facilities and associated "Protection Strategies" based on the assets located at a given facility. The Design Basis Threat Policy separates "Threat Levels" into two distinct categories. One category of "Threat Levels" covers theft, disruption of mission, and espionage and foreign intelligence collection, and the second category - of "Sabotage Threat Levels" - covers radiological, chemical, and biological sabotage.

Five "Threat Levels" are established for theft, disruption of mission, and espionage and foreign intelligence collection: Threat Level 1 (the highest) – for facilities that receive, use, process, store, transport, or test Category IA assets (i.e., nuclear weapons, nuclear test devices, or completed nuclear assemblies) through Threat Level 5 (the lowest) – for facilities that are only

required to maintain minimum safeguards accountability or security operations (i.e., small office activities, tenants in large office buildings, or small isolated research or test facilities that do not possess quantities of special nuclear material).

Four "Sabotage Threat Levels" are established for radiological, chemical, and biological sabotage. Sabotage Threat Level 1 (the highest) through Level 4 (the lowest) are set for facilities, buildings, or operations that process, store or transport radiological, chemical, and biological materials by the degree to which these materials, if dispersed, would result in acute dose effects at the site boundary.

Immediately following the events of September 11, 2001, the Department implemented measures to augment safeguards and security for the most critical Departmental assets. The recently revised Department of Energy Design Basis Threat Policy incorporates those measures and, in some cases, sets a higher standard for the protection of Departmental assets.

The revised Design Basis Threat Policy is effective immediately and will be implemented over the next several years. Actions to augment existing safeguards and security programs for those facilities and assets that are considered the highest security policy will be undertaken as soon as practicable.

That concludes my prepared testimony. Thank you for the opportunity to appear before the Committee. I'll be happy to answer questions.